Data Breach Response Plans : A Guide for Parents / Guardians

Data breaches are serious issues and can have a number of clear impacts on the Trust :

- financial
- reputational
- criminal / legal

.... but more importantly the wellbeing and safety of staff and pupils.

It is therefore important that we minimise the potential for these to occur. We use the following methods to minimise the chances of data breaches occurring :

- training for all staff
- clear processes
- published guidance
- compliance standards for academies
- reviews of incidents
- advisory notes to Principal's

We also recognise that not all data related incidents are the same. So, for internal monitoring we use three categories of data breach which reflect more accurately the nature of any loss as well as the potential response. These categories are :

Data Breach : Loss of data / data incident requiring a referral to the ICO

Data Loss : Data loss / incident requiring referral by an academy to the DPO, but after consideration is not requiring of referral to the ICO but still constitutes internal reviews, responses and possible actions

Data Occurrence : A data 'event' that is not the fault of an individual academy /person, will have little impact and does not require any significant response

Response Plan for Data Breach / Loss

The flowchart above does not give full details as to what is undertaken at each stage of the response. This only outlines the process. Each step has a number of requirements.

Recording Our Decisions
The recording of any incident is key to our professional integrity and ensuring we keep personal data safe. Our record of the incident will include :

- Name Of The Person Referring The Incident
- The Academy / Service
- Date And Time The Issue Was Discovered
- Date And Time The Issue Was Reported
- A Copy Of The Referral Form
- An Analysis Of The Impact :
    - Scale
    - Content
    - Potential
    - Reputational Risk
- Copies Of Email Exchanges
- Immediate Responses Required
- Recommended Follow Up
- Those Involved In The Decision
- Category Of Incident

Will Parents be Notified ?
We will always notify parents when their child, or their own data, has been subjected to a data incident. We will always be open and transparent about what has happened, why it has happened and what we are doing to resolve the matter. Should it be necessary to refer the matter to the ICO then you will also be notified of their recommendations and response. The decision will also be recorded in our internal records.

Referring to the Information Commissioner
From 25 May 2018, if we experience a personal data breach we need to consider whether this poses a risk to people. We need to consider the likelihood and severity of any risk to people's rights and freedoms, following the breach. The decision as to whether we will or not will be taken by the Trust's senior staff based on the advice and recommendations of the DPO. When we've made this assessment, if it's likely there will be a risk then we must notify the ICO; if it's unlikely then we don't have to report it. We do not need to report every breach to the ICO.

What If You Are Not Satisfied With the Response of the Trust to An Incident ?
You always have the right to contact the Information Commissioner to seek advice or make a complaint. Details of how to contact them can be found on our website.

How Will We Know That The Trust Has Had An Incident ?
Our website will contain details of the number of incidents in any academic year. It will also detail the number of referrals to the ICO. You will only find out the details of a specific incident if your personal data has been affected.

This Edition June 2021